July 3, 2024

Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
245 Murray Lane
Washington, D.C. 20528-0380

Re: RIN 1670–AA04

Submitted electronically via http://www.regulations.gov

Dear Director Easterly:

The Workgroup for Electronic Data Interchange (WEDI) writes today in response to the publication of a Notice of Proposed Rulemaking (NPRM) in the April 4, 2024, edition of the *Federal Register* entitled "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements" released by the Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA). In our comments, we will provide feedback specifically on several critical cyber incident reporting issues raised in this NPRM as well as offer our perspectives on a new approach to addressing ransomware enforcement.

WEDI was formed in 1991 by then HHS Secretary Dr. Louis Sullivan to identify opportunities to improve the efficiency of health data exchange. WEDI was named in the HIPAA legislation as an advisor to the Secretary of the Department of Health and Human Services (HHS). Recognized and trusted as a formal advisor to the Secretary, WEDI is the leading authority on the use of health information technology (IT) to efficiently improve health information exchange, enhance care quality, and reduce costs. With a focus on advancing standards for electronic administrative transactions, and promoting data privacy and security, WEDI has been instrumental in aligning the industry to harmonize administrative and clinical data.

General Comments

Ransomware poses a significant and growing threat to the health care industry as well as to other sectors of the economy. Ransomware is unique from other forms of cyberattack, with a specific goal of denying the victim access to their own data, as opposed to removing or copying data, such as a medical record.

In March 2022, President Biden signed CIRCIA into law marking an important milestone for improving America's cybersecurity by, among other things, requiring CISA to develop and implement regulations requiring covered entities to report covered cyber incidents and ransom payments to CISA. It is expected that these reports will facilitate the ability of CISA, in conjunction with other federal partners, to rapidly deploy resources and render assistance to victims suffering attacks, analyze incoming reports across sectors to spot trends and understand how malicious cyber actors are perpetrating their attacks, and quickly share that information with network defenders to warn other potential victims.

Understanding how treacherous the current cyber environment is, we recognize that CISA must have access to accurate information regarding the scope and nature of these cyber-attacks if health care and other sectors are to have any reasonable chance of effectively combating cyberterrorism. Analyzing reports submitted from entities experiencing a cyberattack is expected to facilitate CISA's better understanding of the tactics these criminals are using and what software they are deploying. Having this actionable information will allow the agency to disseminate this critical information to the public and offer guidance to organizations on how to combat current and future cyber threats. Without access to these data, developing and implementing a strategy to counter these criminal acts is far more difficult.

WEDI strongly supports the intent of CIRCIA to address the growing risk of cyberattacks impacting the nation's critical infrastructure sectors, including health care. However, in developing policies and procedures related to cyber incident reporting, we urge CISA to consider the challenges covered entities face during and immediately after experiencing a cyberattack. We counsel CISA to strike the appropriate balance between requiring in a timely manner accurate and comprehensive information from the impacted entity with the need to avoid imposing onerous administrative burdens on organizations while they are experiencing a highly disruptive event.

Specific Comments on the Proposed Rule

WEDI urges CISA to implement an incident reporting process that both meets the needs of a wide array of stakeholder types and is streamlined in such a way that does not overly burden those entities reporting a cyber incident. We make the following comments and recommendations:

CISA Proposal (Pg. 23647)
Section 226.13 of the proposed regulation sets forth the proposed data and records preservation requirements. It includes a recitation of the types of data and records that a covered entity must preserve; the required preservation period; the format or form in which the data and records must be preserved; and the storage, protection, and allowable uses of the preserved data and records.

WEDI Comment
While we appreciate the proposed rule outlining the processes and procedures covered entities must deploy to preserve data and records related to the cyberattack, we urge CISA to include in the final rule information related to how CISA itself will protect and manage the information included in cyber incident reports and supplemental reports

received from covered entities. It is critical that CISA take the steps necessary to protect all information provided by a covered entity in response to CIRCIA reporting requirements and apply the highest level of security controls to prevent this information from being inappropriately accessed. This reported material can include proprietary, sensitive information related to a covered entity's internal network, infrastructure-related information, and security controls. All report information provided to CISA must be kept confidential and not used for any other purpose other than that required under CIRCIA. It could be potentially devastating for the sector if other cyber criminals were to gain access to security data that details IT infrastructure and cybersecurity controls.

Further, we recommend CISA publicly provide additional detail regarding how long submitted data will be stored and how and when it will be disposed along with a confirmation of the disposal to the covered entity.

CISA Proposal (Pg. 23653)
Given the number of existing cyber incident reporting requirements at the Federal and SLTT levels, CISA recognizes that covered entities may be subject to multiple, potentially duplicative requirements to report cyber incidents. In an attempt to minimize the burden on covered entities potentially subject to both CIRCIA and other Federal cyber incident reporting requirements, CISA is committed to exploring ways to harmonize this regulation with other existing Federal reporting regimes, where practicable and seeks comment from the public on how it can further achieve this goal.

WEDI Comment
We strongly urge CISA to align its reporting timelines and requirements with other federal partners, including HHS/Office for Civil Rights, to decrease the administrative burden faced by covered entities potentially required to submit incident reports to multiple agencies. Entities covered under both HIPAA and CIRCIA should only be required to report once, through OCR, to be compliant under both rules, per CIRCIA's substantially similar reporting exception. We also recommend that covered entities not be expected to coordinate the sharing of information between federal agencies--CISA should have that responsibility. Further, CISA should coordinate with other appropriate federal agencies to develop cybersecurity information sharing agreements.

CISA Proposal (Pg. 23653)
Accordingly, CISA has sought to balance the critical need for timely reporting with the potential challenges associated with rapid reporting in the aftermath of a covered cyber incident. For example, CISA recognizes that covered entities may require some limited time to conduct preliminary analysis before establishing a reasonable belief that a covered cyber incident has occurred and thereby triggering the 72- hour timeframe for reporting.

WEDI Comment
Cyberattacks are disruptive and confusing for the entities experiencing them. We continue to believe that for many victims of these types of attacks it could take more than 72 hours to fully identify all the data elements required for the initial report. Our recommendation is that CISA add flexibility to this requirement-permitting covered entities to submit an initial report to the best of their ability within 72 hours while allowing updates to be submitted as

more information and analysis become available.

Further, we urge CISA to recognize the challenges smaller covered entities will face when reporting cyber incidents. Smaller providers, health plans and other types of covered health care entities may not have IT staff trained to recognize when there has been a "substantial cyber incident" that warrants a CIRCIA report. Also, many smaller organizations outsource their IT and security services. With this in mind, we recommend CISA be flexible and that that the 72 hour "clock" (when the initial incident report is to be submitted) start only when the reporting entity has definitively established that a substantial cyber incident has taken place.

CISA Proposal (Pg. 23678)
CISA anticipates that the process for an entity to determine if it is within a critical infrastructure sector will usually be a relatively straightforward exercise. CISA has strong public-private partnerships with the critical infrastructure community, and will be leveraging these relationships as part of the outreach and education campaign that is required by CIRCIA to inform entities that are likely covered entities of the regulatory reporting requirements associated with this proposed rule. CISA expects that entities will be able to obtain informational materials as part of this outreach and education campaign that will simplify the process of determining whether an entity is a covered entity.

WEDI Comment
We are very pleased to see recognition in the NPRM that CISA will be taking a leadership role in educating covered entities regarding reporting requirements specifically and, we anticipate, improving cyber hygiene generally. Reporting a cyber incident to a federal authority is a new process for covered entities. Covered entities, especially smaller organizations, will require training on the new reporting requirements and the reporting process itself. We recommend CISA work with its federal partners, including HHS, as well as private sector organizations such as WEDI to develop educational resources and outreach opportunities to better prepare the health care industry.

CISA Proposal (Pg. 23680)
The first factor Congress identified in 6 U.S.C. 681b(c)(1) is the consequences that disruption to or compromise of an entity could cause to national security, economic security, or public health and safety. While size is not alone indicative of criticality, larger entities' larger customer bases, market shares, number of employees, and other similar size- based characteristics mean that cyber incidents affecting them typically have greater potential to result in consequences impacting national security, economic security, or public health and safety than cyber incidents affecting smaller companies. For example, a successful cyber incident affecting a national drug store chain is much likelier to have significant national security, economic security, or public health and safety impacts than a similar incident affecting a "mom-and- pop" drug store. Similarly, there is a substantially higher likelihood of significant impacts resulting from a successful cyber incident affecting a large industrial food conglomerate, a multinational hotel chain, or a large hospital system than one affecting a small independent farm, a single- location bed and breakfast, or a small doctor's office, respectively.

WEDI Comment
For the health care sector, there is a clear challenge in defining who should be a "covered entity" in terms of cyber incident reporting. We appreciate CISA's inclusion of size as a factor in determining who should be a covered entity. In the NPRM, CISA includes the example cited above, comparing a "large hospital system" and a "small doctor's office," with the former being required to report a covered cyber incident and latter not required to report. There are, however, significant differences in size between the examples cited by CISA and many organizations that would fall between.

We note that there are numerous ways of measuring the size of health care organizations. For providers, these include annual revenue, number of patients treated, number of full-time equivalent clinicians, number of beds (for inpatient facilities). Health plans can be differentiated by annual revenue, number of covered lives, percentage of covered lives in a state or region, and other ways. Health care vendors can be measured by annual revenue, number of clients, geographic market strength, and others.

Adding to the challenge for those in the health care sector of determining who should be required to report a covered cyber incident, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) also uses the term "covered entity" when determining what entity is required to comply with its privacy and security provisions. With this as the backdrop, and prior to finalization of the regulation, we recommend that CISA work with individual health care stakeholder organizations to determine the appropriate definition of covered entity.

CISA Proposal (Pg. 23706)
CISA is proposing to include the second reporting requirement, the requirement for a covered entity to report a ransom payment it has made, in §226.3(b).

WEDI Comment
For health care covered entities that are experiencing a ransomware attack, it is extremely challenging to decide whether to pay the ransom. Cyber criminals not only hold health information hostage, but the attack could also impact the care delivery process and even endanger patient safety. The hope is that paying the ransom will result in the entity being able to return to normal operations. At the same time, covered entities that are attacked know all too well that there is no guarantee that the cyber criminals will unlock the captive data and that paying a ransom could also have the unintended effect of encouraging other cyber criminals. Understanding this dilemma, we urge that CISA and its federal partners to develop guidance to covered entities, based on lessons learned from those that have experienced a ransomware attack, on the pros and cons of paying the ransom demanded.

CISA Proposal (Pg. 23707, 23709-23710)
The first scenario resulting in the requirement to submit a Supplemental Report is when substantial new or different information becomes available to a covered entity. As with the covered cyber incident reporting requirement described above, CISA interprets this requirement as applying to an entity that is a covered entity during any point in the incident lifecycle, such that any entity that qualifies as a covered entity for the purposes of the covered cyber incident reporting requirement is also subject to the supplemental reporting requirement to the extent new or different information becomes

available….CIRCIA requires Supplemental reports be submitted "promptly," which CISA interprets as within 24 hours of the triggering event.

WEDI Response
We strongly support the rule's proposal to permit and encourage the submission of supplemental reports. However, we disagree with the CIRCIA interpretation requiring this supplemental information to be reported within 24 hours of the triggering event. Cyber incidents are rarely straightforward, and an entity's understanding of the incident can evolve as additional information comes to light. This is even more likely with the proposed 72-hour timing requirements for the impacted entity to submit the initial report. The process should, in fact, encourage reporting entities to revise their earlier reports as they learn additional details regarding the incident, and provide them with the time necessary to complete that process. Those entities forced to rush to complete reports (at the same time as they are working to restore internal systems and mitigate potential harm) will likely not include all potentially relevant information. CISA should consider establishing the same timelines for the submission of supplemental reports (i.e., 72-hours after identification of the new information) or permit the impacted entity to apply for an extension and handle these requests on a case-by-case basis.

The overall goal of the reporting process should not just be to have information flow quickly to CISA, but to have complete, accurate, and actionable information flow. All timelines established in the final rule should be long enough to accommodate complex situations where reporting entities face challenges in collecting initial and supplemental information.

CISA Proposal (Pg. 23714-23715)
On balance, CISA believes that the web-based form is the most useful and cost-effective manner for the submission and receipt of CIRCIA Reports and is proposing that as the sole explicitly identified option for submission of CIRCIA Reports.

In light of these drawbacks, CISA is not proposing to include telephonic reporting as a primary option. CISA does, however, intend to maintain telephonic reporting capabilities as a back-up option in case a covered entity is unable to submit a CIRCIA Report using the web-based form for some legitimate reason, such as an outage affecting the availability of the web-based form.

WEDI Response
WEDI strongly supports the proposal to offer a web-based reporting process. Options should include an online web portal and mobile application. Both should offer the ability of the user to save the information they have entered in case they need to stop at some point and come back to the form later (allowing the covered entity to conduct additional internal research or have discussions with colleagues). To support this process, we urge CISA to create a unique reference number to aid the reporting entity when they return to include updated information. The goal should be to reduce the reporting burden as much as possible and have the streamlined process serve as an incentive for those to report a cyber incident.

Most importantly, the incident reporting process must be straightforward and easy to complete for those covered entities reporting. Ease of completion can be achieved by

including comprehensive instructions that can be reviewed prior to starting the process, leveraging drop-down menus as opposed to free-form exposition as much as possible, and limiting the number of questions to the minimum required to achieve the purpose of the reporting.

We also recommend that CISA make available sample cyber incident reports highlighting entities from different stakeholder sectors, different sizes, and reporting different types of cyber incidents. These sample reports would offer guidance for the type of reporting that a covered entity would be expected to provide.

CISA Proposal (Pg. 23721)
First, proposed §226.8(c) would require the submission of information on the vulnerabilities exploited, including but not limited to the specific products or technologies and versions in which the vulnerabilities were found. Next, proposed §226.8(d) would require the submission of information on the covered entity's security defenses, including but not limited to any controls or measures that resulted in detection or mitigation of the incident… As part of this, CISA is likely to ask what, if any, security controls or control families (e.g., NIST Special Pub 800–171 controls; NIST Cybersecurity Framework measures; CISA activities) the covered entity had in place on the compromised system, and, to the extent known, which controls or control families failed, were insufficient, or not implemented that may have been a factor in this incident. CISA also is likely to include questions aimed at helping CISA understand how the covered entity identified the incident; what, if any, detection methods were used to discover the incident; and if the covered entity has identified the initially affected device(s). Finally, proposed §226.8(e), (f) and (g) would require information on the type of incident (e.g., denial-of-service; ransomware attack; multi-factor authentication interception); the TTPs used to cause the incident, to include any TTPs that were used to gain initial access to the covered entity's system; indicators of compromise observed in connection with the covered cyber incident; and a description and copy or sample of any malicious software the covered entity believes is connected with the covered cyber incident.

WEDI Comment
We have concerns regarding some of the information required to be reported related to vulnerabilities, security defenses, and tactics, techniques, and procedures (TTPs). Requiring an impacted entity to reveal confidential and highly sensitive data regarding specific aspects of their information security processes, including specific security controls implemented, broken, or not in place could be counterproductive. Requiring the impacted entity to provide a comprehensive list of an organization's security posture is risky without knowing how that information would be stored and used.

WEDI does not support making questions regarding mitigation and response activities a covered entity is taking or has taken in response to a covered cyber incident required. We believe these questions should be optional and the organization can respond if appropriate. The level of detail and specificity proposed as part of the reporting process also serves to emphasize the challenge of meeting the proposed 72-hour initial reporting window and the 24-hour reporting window for submitting supplemental reports. Health care entities experiencing a cyberattack should be encouraged to focus on ensuring the high-quality delivery of patient care, the preservation of patient safety, and the effective continuation of business operations. These should be the primary focus areas for the

impacted entity, not spending valuable time and resources to meet arbitrary reporting timelines.

To assist covered entities, we encourage CISA to develop guidance on a wide array of cyber incident reporting issues. These should include how covered entities can recognize when a cyber incident has occurred, how to identify when the "clock" has started for the 72-hour deadline for reporting covered cyber incidents and for the 24-hour deadline for reporting ransom payments, what information the covered entity is required to collect, report and retain, and other relevant topics.

Cyberattacks are rarely straightforward and for many covered entities, they will have no prior experience dealing with this type of traumatic incident. We recommend establishing a two-year enforcement discretion period following publication of the final rule to allow for CISA, its federal partners, and the private sector to educate covered entities and an ongoing "grace period" to the 72-hour deadline for reporting covered cyber incidents and for the 24-hour deadline for reporting ransom payments before taking any enforcement action.

CISA Proposal (Pg. 23727)
As discussed above, CISA is proposing that covered entities or third parties submitting CIRCIA Reports on behalf of a covered entity are required to do so using the web-based user interface or other mechanism subsequently approved by the Director.

WEDI Comment
In terms of the data reported by impacted entities, it will be critical for CISA to ensure this reported information is kept secure. To be comprehensive, the reporting process is likely to collect data pertaining to patient health information and internal security policies and procedures. As we have indicated, these reports can contain sensitive information and we recommend CISA provide assurances to impacted entities directly on the web-based reporting tool that any information collected by the agency will be kept strictly confidential.

To reiterate, CISA should deploy measures appropriate to maintain a high level of security for both the data being reported via the web and all data collected. We recommend CISA include in the reporting instructions the steps the agency is taking to ensure the security of the data is maintained and all associated privacy policies and procedures. We also recommend CISA specify how the reported data will be used, who will have access to the information, and how long the information will be retained.

CISA Proposal (Pg. 23728)
CIRCIA authorizes covered entities to use third parties to submit Covered Cyber Incident Reports or Ransom Payment Reports on behalf of the covered entity. Specifically, 6 U.S.C. 681b(d)(1) states "[a] covered entity that is required to submit a covered cyber incident report or a ransom payment report may use a third party, such as an incident response company, insurance provider, service provider, Information Sharing and Analysis Organization, or law firm, to submit the required report under subsection (a)."

WEDI Comment
We strongly concur with the rule proposing to permit third parties to submit reports to CISA on behalf of a covered entity. We anticipate that many covered entities, especially

smaller organizations, will utilize the services of IT and security third parties. We also concur with the requirement that the third party show proof that they have permission to act on behalf of the covered entity. However, we believe that while the covered entity should be required to include in its report that a third party was involved in the detection of the cyber incident, the mitigation of the incident, and/or the reporting of the incident, these third parties should be under no legal obligation to report a cyber incident independent of the covered entity.

CISA Proposal (Pg. 23731)
CISA is aware that retaining data and records is not without cost… CISA is proposing that covered entities that submit CIRCIA Reports must begin preserving the required data at the earlier of either (a) the date upon which the entity establishes a reasonable belief that a covered cyber incident has occurred, or (b) the date upon which a ransom payment was disbursed, and must preserve the data for a period of no less than two years from the submission of the latest required CIRCIA Report submitted pursuant to §226.3, to include any Supplemental reports.

WEDI Comment
We understand the interest on the part of CISA, and potentially other enforcement agencies, in having access to pertinent information regarding a cyberattack after the event has occurred. However, we are concerned that the requirement for a covered entity to retain all information related to the attack for two years is excessive. The information required to be maintained not only includes electronic files such as Word documents but could also include paper records and information stored in multiple electronic formats. As CISA acknowledges, this information retention process will be intrusive and costly. As covered entities will already be dealing with the economic impact of the attack itself, we urge CISA to require covered entities to retain this information for no more than 1 year after the date of submission of either the initial or supplemental report, whichever is later.

CISA Proposal (Pg. 23733)
Pursuant to 6 U.S.C. 681d(e), CISA must consider certain factors when determining whether to exercise any of these enforcement authorities. Specifically, CIRCIA mandates the Director take into consideration the complexity of determining whether a covered cyber incident occurred, and the covered entity's prior interaction with CISA or its understanding of the policies and procedures for reporting for covered cyber incidents and ransom payments, as part of the process for evaluating whether to exercise an enforcement mechanism.

WEDI Comment
Cyberattacks present a danger to all health care entities and the patients they serve. When addressing these attacks, the current enforcement approach creates a culture of "blaming the victim." We would argue that this approach should be changed to one focused on transparency and action. This revised approach will lead to improved critical sector cyber hygiene and a reduced threat to patient records and patient safety specifically in the health care sector. As evidenced by recent attacks on health care, when an organization is cyberattacked not only is care coordination and data sharing impacted, but in some cases patient safety can be threatened.

Typically, a ransomware attack will encrypt an organization's data with a key known only to the hacker who inserted the malware. The hacker then demands a ransom be paid to release the data through use of a decryption key. In many cases, the perpetrator will instruct the victim to pay a ransom via an untraceable cryptocurrency, such as Bitcoin. In some cases, the health care sector has seen these criminals deploy ransomware with the goal of damaging or destroying patient data. Ransomware is therefore distinct from other breach-type events where protected health information (PHI) has been improperly disclosed to unauthorized individuals.

The federal government currently considers a ransomware attack a "data breach," and thus entities attacked by ransomware are subject to the same process for both notification and enforcement as laid out in the breach notification provisions included in the 2013 HIPAA Omnibus regulation. We assert, however, that this equating of ransomware with a traditional breach of PHI is inappropriate. It is unreasonable and counter-productive for an entity to be penalized by the federal government for a ransomware attack that is beyond their control. We are concerned that the threat of punitive measures being imposed by the federal government following a ransomware attack could act as a deterrent against reporting the event.

It is unreasonable and counter-productive for covered entities to be penalized by the federal government for a ransomware attack that is beyond their control. We are concerned that the threat of punitive measures being imposed by the federal government following a ransomware attack could act as a deterrent against reporting the event. It is also important to note that organizations experiencing a ransomware attack incur significant harm from the attack itself. The inability to access important data that an organization maintains can be catastrophic in terms of the lock out of sensitive patient information, disruption to regular operations (including the ability to treat patients), financial losses related to lost claims data, the expense incurred to restore systems and files, and the potential long-term harm to the reputation of the organization.

Ransomware is not typically a use or disclosure of PHI but rather extortion to unlock or regain access to data critical to the business. This new, insidious form of attack on our nation's health care delivery settings demands a new approach to information gathering and enforcement action. Therefore, we urge the federal government to adopt a ransomware policy that encourages covered entities to report cyberattacks and collaborate with the federal government in an investigation to mitigate the damage and ensure the safety of its patients.

We strongly recommend the federal government institute a policy to establish that ransomware is not considered a data breach when the covered entity has deployed a recognized security program and when no PHI has been accessed. Should no breach of the data occur that results in data being accessed by unauthorized entities and the covered entity be found to have a made good faith effort to deploy a recognized security program and instituted security policies and procedures, the covered entity should not be deemed to have experienced a data breach.

CISA Proposal (Pg. 23737)
Specifically, CISA proposes under the first category, Treatment of Information, the following protections which are consistent with 6 U.S.C. 681e: (a) Designation as

Commercial, Financial, and Proprietary Information, (b) Exemption from Disclosure under FOIA, (c) No Waiver of Privilege or Protection Provided by Law, and (d) an Ex Parte Communications Waiver.

WEDI Comment
We assert that one of the foundations to the final rule should be protection of privacy and civil liberties. We recommend CISA apply appropriate privacy and civil liberty protective measures over covered entities' data, submitted voluntarily or through subpoena under the Cyber Incident Reporting Rule, through a FOIA request, requests from federal or state governments for information, legal discovery (including criminal or civil litigation), and for other purposes. The NPRM only describes this protection for voluntarily submitted reports, but not those submitted through subpoena. There might be circumstances where the covered entity may be forced to divulge their cybersecurity incident, and they should not be re-victimized by the government.

Conclusion

We appreciate the opportunity to share with CISA our perspectives on cyber incident reporting and ransomware issues. CISA has the important task of developing a cyber incident reporting process that meets the needs of a wide variety of covered entities. To decrease the burden for those required to report, we urge CISA to continue to work with other federal agencies to create a single federal cyber incident reporting procedure. We also recommend partnering with the appropriate public and private sector organizations to educate covered entities on how best to avoid cyber incidents and how to report them should one occur.

Please contact Charles Stellar, WEDI President & CEO, at cstellar@WEDI.org to discuss these comments or explore opportunities to work together to educate health care stakeholders.

Sincerely,
/s/
Ed Hafner
Chair, WEDI

cc: WEDI Board of Directors